# UNITED STATES PATENT AND TRADEMARK OFFICE

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/786,224 | 02/26/2004 | Burkhard Kuhls | 080437.53236US | 2832 |

23911            7590            06/21/2011
CROWELL & MORING LLP
INTELLECTUAL PROPERTY GROUP
P.O. BOX 14300
WASHINGTON, DC 20044-4300

| EXAMINER |
|---|
| JOHNSON, CARLTON |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2436 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 06/21/2011 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

|  | Application No. | Applicant(s) |
|---|---|---|
| **Office Action Summary** | 10/786,224 | KUHLS, BURKHARD |
|  | Examiner | Art Unit |  |
|  | CARLTON JOHNSON | 2436 |  |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *17 March 2011*.

2a)☐ This action is **FINAL**.    2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1,3-9 and 12-20* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-9 and 12-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All  b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

## DETAILED ACTION

1.    In view of the Appeal Brief filed on 3/17/2011, PROSECUTION IS HEREBY

REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of

the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a

reply under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be

accompanied by a supplemental appeal brief, but no new amendments, affidavits

(37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR

1.193(b)(2).

A Supervisory Patent Examiner (SPE) has approved of reopening

prosecution by signing below:

/Nasser  Moazzami/

Supervisory Patent Examiner, Art Unit 2436.


2.    Claims **1, 3 - 9, 12 - 20** are pending.   Claim **2, 10, 11** have been

cancelled.   Claims **1, 7, 19** are independent.    The application was filed on 2-26-

2004.


### *Response to Arguments*

3.    Applicant's arguments have been fully considered and they were not

persuasive.   New grounds of rejection have been entered.

3.1    Applicant argues on pages 6, 9, 13 of Remarks *that for Claim 1 the*

*referenced prior art does not disclose all of the claim limitations*:

*1. The Combination of England, Ishii and Wong Does not Disclose or Suggest*

*Generating a Software Signature Certificate in the Manner Required by Claim 1;*

*2. The Combination of England, Ishii and Wong Does not Disclose or Suggest*

*Checking a Software Signature Certificate in the Manner Required by Claim 1;*

*3. The Combination of England, Ishii and Wong Does not Disclose or Suggest*

*Checking Signed Software for Integrity in the Manner Required by Claim 1.*

The Examiner disagrees.   England, Ishii, and Wong are no longer used as

grounds of rejection.

Schmidt discloses the limitations of claim 1:

Schmidt discloses: *generating a software signature certificate using the public*

*key of the software signature site and a secret key of a control entity,*

*according to a public-key method.*  (see Schmidt paragraph [0059], lines

6-10: generates key pair and sends public key with certificate request;

paragraph [0060], lines 1-4: trust center (control unit) generates certificate,

signs by means of secret key (trust center) and sends to certificate holder;

paragraph [0012], lines 6-9: trust center analogous to vehicle, control

unit))

Schmidt discloses generating a certificate and sending the public key
along with a request to sign the certificate. And, Schmidt discloses
signing the certificate using a private key of a trust center. Schmidt
discloses that a trust center can be the same as a control unit for a
vehicle.

Schmidt discloses: *wherein prior to execution of the software, by the control
unit, signing the software against falsification, using a secret or private key
of a software signature site, according to a public-key method.* (see
Schmidt paragraph [0014], lines 1-6: sign software to be imported into the
control unit, by means of the second (private) key of the pair of certificate
keys)
Schmidt discloses signing software before the software is imported or
loaded into a vehicle control unit. Schmidt discloses that the software is
signed with a secret (private key).

Schmidt discloses: *checking the signed software signature certificate for
integrity, according to a public key method using a public key of the trust
center.* (see Schmidt paragraph [0014], lines 6-11: by means of this first
(public) key of the key pair, the signature of the imported software is
checked)
Schmidt discloses using a public key of a certificate key pair to check a
signed certificate.

Schmidt discloses: *checking the signed software for integrity, using a public key of the software signature site contained in the software signature certificate, the public key of the software signature site being complementary to the secret key of the software signature site.* (see Schmidt paragraph [0068], lines 1-3: certificate verified as faultless; checked in next step whether software is properly signed, the public key from the certificate is used)

Schmidt discloses checking to verify the integrity of a digital signature for a software program product. The digital signature is checked using the public key of the certificate.

3.2    The Office Action addresses the additional arguments on pages 17 and 19 for Claims 7 and 19 indicated by Applicant.

3.3    Applicant argues on pages 21 of Remarks that dependent claims 3 - 6, 8, 9, 12 - 18 and 20 are allowable by virtue of their dependence on independent claims.

The Examiner disagrees since the arguments against the dependent claims are answered by responses to the independent claims.

## Claim Rejections - 35 USC § 102

4.      The following is a quotation of the appropriate paragraphs of 35 U.S.C.

102 that form the basis for the rejections under this section made in this Office

action:

> A person shall be entitled to a patent unless -
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5.      Claims **1, 3 - 20** are rejected under 35 U.S.C. 102(e) as being anticipated

by **Schmidt et al.** (US PGPUB No. **20020023223**)


**Regarding Claim 1**, Schmidt discloses a method comprising providing software

for use by a control unit;

a) generating a software signature certificate using the public key of the

   software signature site and a secret key of a control entity, according to a

   public-key method,  (see Schmidt paragraph [0059], lines 6-10: generates

   key pair and sends public key with certificate request; paragraph [0060],

   lines 1-4: trust center (control unit) generates certificate, signs by means

   of secret key (trust center) and sends to certificate holder; paragraph

   [0012], lines 6-9: trust center analogous to vehicle, control unit))

Furthermore, Schmidt discloses the following:

b) wherein prior to execution of the software, by the control unit, signing the

   software against falsification, using a secret or private key of a software

   signature site, according to a public-key method; (see Schmidt paragraph

   [0014], lines 1-6: sign software to be imported into the control unit, by

means of the second (private) key of the pair of certificate keys)

c) checking the signed software signature certificate for integrity, according to

a public key method using a public key of the trust center; (see Schmidt

paragraph [0014], lines 6-11: by means of this first (public) key of the key

pair, the signature of the imported software is checked)

d) checking the signed software for integrity, using a public key of the

software signature site contained in the software signature certificate, the

public key of the software signature site being complementary to the

secret key of the software signature site; (see Schmidt paragraph [0068],

lines 1-3: certificate verified as faultless; checked in next step whether

software is properly signed, the public key from the certificate is used)

**Regarding Claim 3**, Schmidt discloses the method according to claim 1, wherein

one of a control entity certificate and a trust center certificate is generated

according to a public-key method by using the secret key of the control entity.

(see Schmidt paragraph [0019], lines 4-7: public key (key pair: public, private) of

control unit can be filed in control unit (stored); signature to be checked must be

formed by means of secret (private) key)

**Regarding Claim 4**, Schmidt discloses the method according to claim 1, wherein

clearing code data are signed using a secret key of a clearing code site

according to a public key method. (see Schmidt paragraph [0024], lines 4-10:

using means of a secret (private) key a digital signature can be generated for a

document (certificate, software); authenticity of document (certificate, software)

checked by verification of signature by using public key)


**Regarding Claim 5**, Schmidt discloses the method according to claim 1, wherein

a clearing code site signature certificate is generated using the secret key of the

control entity of the trust center according to a public-key method.  (see Schmidt

paragraph [0024], lines 4-10: using means of a secret (private) key a digital

signature can be generated for document (certificate, software); authenticity of

document (certificate, software) can be checked by verification of signature by

using public key)


**Regarding Claim 6**, Schmidt discloses the method according to claim 3, wherein

the trust center certificate is protected against falsification and exchange, in a

protected memory area in the control unit.  (see Schmidt paragraph [0020], lines

1-4; paragraph [0021], lines 1-6: secret keys are filed within certificate

information in control unit; key information filed (stored) in control unit are filed in

boot sector (and protected in a special manner); boot sector can also be

constructed such that it is blocked against future access (write access))


**Regarding Claim 7**, Schmidt discloses a method of providing software for use by

a control unit of a vehicle, said method comprising:

   a)  before its use by the control unit, signing the software against falsification

       (see Schmidt paragraph [0014], lines 1-6: sign software to be imported

into the control unit)

Furthermore, Schmidt discloses the following:

b) checking the signed software for integrity, using a public key

complementary to the secret key of the software signature site; (see

Schmidt paragraph [0014], lines 6-11: by means of this key (first or public)

key of the pair, the signature of imported software is checked)

wherein a clearing code site signature certificate, a software signature

certificate, the clearing code data and their signature as well as the

software and its signature are stored in the control unit; (see Schmidt

paragraph [0020], lines 1-4: secret keys are filed within certificate

information in the control unit; paragraph [0018], lines 1-11: when several

certificates are use, signature of first certificate check by key filed in

control unit, each certificate is checked)

wherein generating a signature certificate using the public key of the

signature site and a secret key of a control entity, according to a public-

key method. (see Schmidt paragraph [0059], lines 6-10: generates key

pair and sends public key with certificate request; paragraph [0060], lines

1-4: trust center (control unit) generates certificate, signs by means of

secret key (trust center) and sends to certificate holder; paragraph [0012],

lines 6-9: trust center analogous to vehicle or control unit)


**Regarding Claim 8**, Schmidt discloses the method according to claim 1, wherein

the software signature certificate includes at least one validity restriction. (see

Schmidt paragraph [0026], lines 1-6: control unit of a specific vehicle contains vehicle specific information such as a chassis number or other vehicle-specific data; specification on page 3, paragraphs [0011], paragraph [0012} discloses a validity restriction such as a restriction to a control unit which is specified; (vehicle specific data))

**Regarding Claim 9**, Schmidt discloses the method according to claim 5, wherein the clearing code site signature certificate includes at least one validity restriction, a restriction to a particular control unit which is designated by means of an identification number stored in the control unit in an invariable manner, and a restriction to an identification number. (see Schmidt paragraph [0026], lines 1-6: control unit of a specific vehicle contains vehicle specific information such as a chassis number (identification number) or other vehicle-specific data)

**Regarding Claim 12**, Schmidt discloses the method according to claim 5, wherein the clearing code site signature certificate is checked for integrity according to a public key method, using a public key of the trust center. (see Schmidt paragraph [0023]; paragraph [0024], lines 7-10: secret key can be used to generate a valid signature; authenticity of signature for software can be checked by using public key)

**Regarding Claim 13**, Schmidt discloses the method according to claim 4, wherein the signed clearing code data are checked for integrity according to a

public key method, using a public key of the clearing code site contained in the

clearing code site signature certificate. (see Schmidt paragraph [0023];

paragraph [0024], lines 7-10: secret key can be used to generate a valid

signature; authenticity of signature for software can be checked by using public

key)

**Regarding Claim 14**, Schmidt discloses the method according to claim 1,

wherein the control unit is equipped with a sequence-controlled microprocessor

that implements one of the above-described methods. (see Schmidt paragraph

[0044], lines 1-8: software determines the functionality of control unit housed in

programmable memory; different types of microcomputers used depending on

control unit; 8-bit, 16-bit, or 32-bit processor)

**Regarding Claim 15**, Schmidt discloses a control unit, which implements a

method according to claim 1. (see Schmidt paragraph [0044], lines 1-8: software

determines the functionality of control unit housed in programmable memory;

different types of microcomputers used depending on control unit; 8-bit, 16-bit, or

32-bit processor)

**Regarding Claim 16**, Schmidt discloses a data processing system, which

implements a method according to Claim 1. (see Schmidt paragraph [0044], lines

1-8: software determines the functionality of control unit housed in programmable

memory; different types of microcomputers used; 8-bit, 16-bit, or 32-bit

processor)

**Regarding Claim 17**, Schmidt discloses a computer program product sequence control of a data processing system, which implements the method according to Claim 1. (see Schmidt paragraph [0044], lines 1-8: software (computer program product) determines the functionality of control unit housed in programmable memory; different types of microcomputers used depending on control unit)

**Regarding Claim 18**, Schmidt discloses a data carrier, comprising a computer program product according to claim 17. (see Schmidt paragraph [0044], lines 1-8: software (computer program product) determines the functionality of control unit housed in programmable memory; different types of microcomputers used depending on control unit)

**Regarding Claim 19**, Schmidt discloses a method of providing software for use by a control unit of a vehicle, said method comprising:

   a) storing, a software signature certificate; (see Schmidt paragraph [0060], lines 1-4: generate certificate, signs it and sends it back to certificate holder where it remains (stored))

Furthermore, Schmidt discloses the following:

   b) receiving, by the control unit, signed software; (see Schmidt paragraph [0061], lines 6-10: signed software and certificate are imported into a vehicle (control unit))

c) checking, by the control unit, whether the software signature certificate has been changed or manipulated; (see Schmidt paragraph [0067], lines 1-5: examined by means of public key stored in control unit whether signature of certificate is faultless (not been changed); paragraph [0067], lines 12-14: in indicated example, certificate has been changed in an unauthorized manner)

c) checking, whether the signed software has been changed or manipulated. (see Schmidt paragraph [0068], lines 1-6: certificate is verified as faultless; check whether software is properly signed; public key from certificate is used to define a hash, which is compared with hash defined directly from software)

**Regarding Claim 20**, Schmidt discloses the method of claim 19, further comprising:

a) storing, a trust center certificate that includes a public key and a signature generated using a secret key of a trust center; (see Schmidt paragraph [0060], lines 1-4: generate certificate, signs it and sends it back to certificate holder where it remains (stored))

Furthermore, Schmidt discloses the following:

b) storing, a clearing code site signature certificate that includes a second public key and a second signature; (see Schmidt paragraph [0060], lines 1-4: generate certificate, signs it and sends it back to certificate holder where it remains (stored))

c) wherein the software signature certificate includes a third public key and a

third signature; (see Schmidt paragraph [0060], lines 1-4: generates

certificate; signs it and sends it (including signature) to certificate holder;

paragraph [0053], lines 1-4: public key is filed as certificate information

within certificate)


### *Conclusion*


Any inquiry concerning this communication or earlier communications from

the examiner should be directed to Carlton V. Johnson whose telephone number

is 571-270-1032. The examiner can normally be reached on Monday thru Friday

, 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the

examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The

fax phone number for the organization where this application or proceeding is

assigned is 571-273-8300.

Information regarding the status of an application may be obtained from

the Patent Application Information Retrieval (PAIR) system. Status information

for published applications may be obtained from either Private PAIR or Public

PAIR. Status information for unpublished applications is available through

Private PAIR only. For more information about the PAIR system, see http://pair-

direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-

free). If you would like assistance from a USPTO Customer Service

Representative or access to the automated information system, call 800-786-

9199 (IN USA OR CANADA) or 571-272-1000.

Carlton V. Johnson
Examiner
Art Unit 2436

CVJ
May 23, 2011

/Nasser  Moazzami/

Supervisory Patent Examiner, Art Unit 2436